



DEPARTMENT OF THE NAVY  
NAVY PERSONNEL COMMAND  
5720 INTEGRITY DRIVE  
MILLINGTON TN 38055-0000

NAVPERSCOMINST 5211.1  
PERS-00J  
12 SEP 2006

NAVPERSCOM INSTRUCTION 5211.1

From: Commander, Navy Personnel Command

Subj: IMPLEMENTATION OF THE PRIVACY ACT (PA) FOR NAVY  
PERSONNEL COMMAND (NAVPERSCOM)

Ref: (a) 5 U.S.C., 522a  
(b) DOD 5400.11-R of Aug 83  
(c) SECNAVINST 5211.5E

Encl: (1) Rules of Conduct Under the Privacy Act  
(2) OPNAV 5211/9, Disclosure Accounting Form

1. Purpose. To implement references (a) through (c); to ensure that all Navy Personnel Command (NAVPERSCOM) members, civilian, and contractor employees are made fully aware of their rights and responsibilities under the provisions of the Privacy Act (PA) to balance the government's need to maintain information with the obligation to protect individuals against unwarranted invasion of their privacy stemming from the Department of the Navy's (DON's) collection, maintenance, use, and disclosure of Protected Personal Information (PPI); and to require that privacy management practices and procedures be employed to evaluate privacy risks in publicly accessible organization Web sites and unclassified non-national security information systems.

2. Cancellation. COMNAVPERSCOM Administrative Manual, Article 0600-0100.

3. Background

a. Reference (a), The Privacy Act of 1974, PL 93-579, implemented by references (b) and (c), requires a number of changes to administrative and operational procedures regarding the handling, maintenance, disposal, and release of personnel records and personal information to the public and to the individual.

b. Major requirements include but are not limited to the following:

(1) All types and kinds of records and documents are to be made available to the individual upon request. ("Record" has a much broader meaning under the PA than usual references. A PA "record" can be a piece of paper with an individual's name or social security number (SSN) on it and one element of personal information that is retrieved by personal identifier and part of a PA System of Record.)

(2) Requests for notification (i.e., information on requester in a particular system of records) and access under the PA should be acknowledged within 10-working days of receipt of the request. (See Requests for Notification and Access to Records in the PA Records System at <http://privacy.navy.mil/privacy/noticenumber/noticeindex.asp>.)

(3) Records requested should be made available to requester within 30-working days of receipt of request. (See Requests for Notification and Access to Records in the PA Records System.)

(4) Only information that is both necessary and relevant may be collected and used concerning any individual. It must be maintained in an accurate, relevant, timely, and complete manner.

(5) Individuals have the right to request amendment of their record. Receipt of the amendment request must be acknowledged within 10-working days of receipt.

(6) Generally, disclosure of personal information, other than to the individual and to officials and employees of agencies established as routine users in the Record Systems Notices published in the Federal Register, is not permitted without the written consent of the individual. Detailed disclosure criteria and information are contained in Release of Information and Accounting of Disclosures.

(7) The following data elements are considered releasable to the public and do not require the written consent of the individual:

(a) Military:

1. Full name

12 SEP 2006

2. Rank/rate and date of rank/rate
3. Gross salary
4. Past duty stations
5. Source of commission
6. Military education
7. Promotion sequence number
8. Duty status
9. General and Special court-martial results
10. Awards, decorations, and citations

(b) Civilian:

1. Full name
2. Grade
3. Date of employment
4. Title of position
5. Gross salary

(8) An accounting of disclosures to those outside Department of Defense (DOD) and agencies not covered by an Inter-Agency Support Agreement (IASS) must be maintained. (See Release of Information and Accounting of Disclosures.)

(9) Appoint a PA Team to identify ways to ensure no inadvertent releases of PPI and establish best business practices.

4. Rules of Conduct and Criminal Liability of Employees. Enclosure (1) specifies the rules of conduct under the PA that are applicable to all officials and employees in DON. Everyone should be thoroughly familiar with these rules of conduct and the criminal liabilities involved. Particular emphasis should

1 2 SEP 2006

be given the fact that the PA provides for criminal sanctions and fines of up to \$5,000 against an official or employee who:

a. Willfully discloses information protected under the PA to an individual or agency not authorized access to it.

b. Willfully maintains a system of records that were not published in the Federal Register.

c. Asks, obtains, or receives personal data under false pretenses.

5. Privacy Act Coordination Office. NAVPERSCOM, Office of Legal Counsel (PERS-00J) serves as the centralized office and point of contact to provide guidance and assistance, where applicable, in administering the Privacy Act of 1974. Overall responsibilities of this office are as follows:

a. Develop overall NAVPERSCOM policy relative to the PA.

b. Monitor compliance with DOD and Secretary of the Navy (SECNAV) PA instructions.

c. Develop materials such as forms, reporting formats, and directives for implementation of the PA. Consolidate data and make required reports, including denials of PA requests. Ensure training programs required by the PA are accomplished. Process requests and maintain processing logs for notification, access, and amendment under the PA. Coordinate with responsible Department PA Coordinators as required, and obtain assistance, when necessary.

d. Provide a brief overview of the PA and provide a copy of the current PA training module to new command personnel during check-in. Provide annual PA Refresher Training material to Department Privacy Act Coordinators for additional Department-level training as applicable.

e. Head the NAVPERSCOM Privacy Team. Meet on a regular basis with Department Privacy Act Coordinators to ensure compliance with the Navy's Privacy Act Program.

**1 2 SEP 2006**

**6. Department Privacy Act Coordinators**

a. Each Assistant Commander, Navy Personnel Command (ACNP) will designate, in writing, a Department PA Coordinator who will function as their department's POC on all PA matters and will be a member of the NAVPERSCOM Privacy Team. The Department PA Coordinators will be the rank of O4 or above or a civilian equivalent grade. This assignment should not be construed as a light collateral duty, but rather as an important component of a department's responsibility to comply with the PA. For the purpose of the PA, Department PA Coordinators report to the NAVPERSCOM PA Coordinator. Specific duties of Department PA Coordinators are as follows:

(1) Respond promptly to requests from NAVPERSCOM (PERS-00J) for access, copies of records, or amendment action concerning records within their respective departments.

(2) Provide annual PA Refresher Training to their department personnel by utilizing PA Training material sent to them by the NAVPERSCOM Privacy Act Coordinator. Provide the NAVPERSCOM Privacy Act Coordinator with the number of their division personnel who completed annual refresher training. The Department Privacy Act Coordinator will ensure that each of their department personnel completes annual PA Refresher Training.

(3) Review and revise, as appropriate, all Naval Military Personnel Manual (MILPERSMAN) articles, instructions, notices, and other manuals under the department's responsibility to meet the requirements of the PA.

(4) Monitor the relevance, accuracy, timeliness, and completeness of records and data elements for which their department is responsible.

(5) Evaluate and designate records within their respective department that meet the criteria of "sensitive" data and ensure such data is stored and disposed of as specified in Safeguarding Personal Information of this instruction.

(6) Ensure that requests for personnel record data are released under current procedures. If Department PA Coordinators are uncertain as to whether or not disclosure of

1 2 SEP 2006

data is authorized under the PA, contact the NAVPERSCOM PA Coordinator for assistance.

(7) Ensure that an accounting of disclosures made to agencies, those outside DOD and with whom IASSs do not exist, is recorded in enclosure (2), and filed in the applicable record. Additional guidance is contained in Release of Information and Accounting of Disclosures.

(8) Draft PA statements for those forms under the department's cognizance that require such statements. Chop through NAVPERSCOM, Records Officer/Forms Manager (PERS-332/332F), as appropriate and NAVPERSCOM (PERS-00J) prior to submitting for printing.

(9) Provide PA Privacy Program guidance to their department personnel who solicit and award or administer government contracts; and inform prospective contractors of their responsibilities regarding the DON PA Program. This activity should be coordinated with the NAVPERSCOM Contract Specialist Subject Matter Expert (SME).

(10) Establish contract surveillance programs for their departments to ensure contractors comply with the procedures established by Defense Acquisition Regulatory (DAR) Council. This activity should be coordinated with the NAVPERSCOM Contract Specialist Subject Matter Expert (SME).

(11) Meet on a regular basis with the NAVPERSCOM Privacy Act Coordinator in order to discuss their department PA issues, provide suggested solutions to PA problems, and provide updates to ongoing PA initiatives.

#### 7. Subject Matter Experts (SMEs)

a. In addition to Department Privacy Act Coordinators, SMEs will also be appointed as part of the NAVPERSCOM Privacy Team. At a minimum, the NAVPERSCOM Privacy Team will include a designated SME representative from NAVPERSCOM, Records Officer (PERS-332), NAVPERSCOM Contract Specialist (PERS-333), and NAVPERSCOM, Information Technology (PERS-34).

12 SEP 2006

## 8. Safeguarding Personal Information

a. The Privacy Act of 1974 requires that certain safeguards be taken to ensure the security and confidentiality of personal information contained in various records systems maintained by NAVPERSCOM.

b. If the inadvertent or unauthorized disclosure of personal information or records will result in substantial harm, embarrassment, inconvenience, or unfairness to an individual, such records must be given proper protection against hazards to their security or integrity.

c. A considerable portion of daily business within NAVPERSCOM involves personal information that can be considered "sensitive" under the PA criteria contained in Safeguarding Personal Information. A determination of what is "sensitive" versus what is "routine" is the responsibility of each department that will be governed by the criteria in Safeguarding Personal Information. Documents containing name in conjunction with SSN, date of birth, address, or other personal information are considered "sensitive" under the PA.

d. Storage. Generally limited access to buildings after working hours will suffice relative to the storage of personnel records, etc. If any records, documents, or listings are in the "sensitive" category, storage must be so that they can not be openly viewed with the exception of material in the selection board area that has other security precautions in effect.

e. Disposal. Per reference (c), PA records must be disposed of by rendering the material unrecognizable or beyond reconstruction (e.g., burning, chemical decomposition, shredding, or mutilation.)

f. All NAVPERSCOM Departments are responsible for meeting the same requirements for determining information category, storage, and disposal.

## 9. Protected Personal Information (PPI)

a. Access/Disclosure. Access to and disclosure of PPI such as SSN, date of birth, home address, home telephone number, etc., must be strictly limited to individuals with an official

need to know. It is inappropriate to use PPI in group/bulk orders. Appropriate actions must be taken to protect PPI from being widely disseminated. In particular, PPI shall not be posted on electronic bulletin boards because the PA strictly limits PPI access to those offices and employees of the agency with an official need to know.

b. Transmittal. In those instances where transmittal of PPI is necessary, the originator must take every step to properly mark the correspondence so that the receiver of the information is apprised of the need to properly protect the information. For example, when transmitting PPI in a paper document, fax, or e-mail, it may be appropriate to mark it "FOR OFFICIAL USE ONLY (FOUO) - PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties." When sending a message that contains PPI, it should be marked FOUO. It is also advisable to inform the recipient that the message should not be posted on a bulletin board. In all cases, recipients of message traffic that contain PPI, whether marked FOUO or not, must review it prior to posting it on an electronic bulletin board.

c. Collection/Maintenance. The collection and maintenance of information retrieved by an individual's name and/or personal identifier should be performed in compliance with the appropriate PA systems of record notice (see <http://www.privacy.navy.mil>). If you need to collect and maintain information retrieved by an individual's name and/or personal identifier, you must have an approved PA systems notice to cover that collection. If you are unsure as to whether a systems notice exists or not, contact the NAVPERSCOM PA Coordinator for assistance.

d. Unauthorized Disclosure. In the event an unauthorized disclosure of PPI is made, Departments shall:

(1) Take immediate action to prohibit further damage/disclosure. The ACNP for the applicable department will immediately notify Commander, Navy Personnel Command (COMNAVPERSCOM) and the NAVPERSCOM PA Coordinator of an unauthorized PPI disclosure.

(2) Within 10 days, COMNAVPERSCOM shall notify all affected individuals by letter, including the specific data involved and the circumstances surrounding the incident. If

COMNAVPERSCOM is unable to readily identify the affected individuals, a generalized notice should be sent to the potentially affected population. As part of any notification process, individuals shall be informed to visit the Federal Trade Commission's (FTC's) Web site at <http://www.consumer.gov/idtheft> for guidance on protective actions the individual can take. A synopsis of the disclosure made, number of individuals affected, actions to be taken, should be e-mailed to Chief of Naval Operations (CNO) (DNS 36) "Identity Theft Notification" in the subject line.

(3) If NAVPERSCOM is unable to comply with the notification requirements set forth in subparagraph (2) above, COMNAVPERSCOM shall immediately inform CNO (DNS 36) as to the reasons why. CNO (DNS 36) will, in turn, notify the Secretary of Defense.

10. Requests for Notification and Access to Records in the PA Records System

a. Any request for notification, access, or copies of records or documents that cite the PA must hand-carry, mail, or e-mail the request for expeditious processing to the NAVPERSCOM PA Coordinator due to time constraints imposed by the Act.

b. Routine requests for copies of records not citing the PA should continue to be handled according to other current instructions.

c. Any requests for access or copies of any documents or records from the individual (not third party requests) and citing the Freedom of Information Act (FOIA) must also be hand-carried, mailed, or e-mailed to the NAVPERSCOM PA coordinator for expeditious handling due to time constraints. FOIA requests from individuals asking for their own records will be treated as PA requests.

d. The NAVPERSCOM PA Coordinator will accomplish processing of correspondence submitted under the PA. This includes sending acknowledgment to the requester, tracking of requests, collecting requested information from responsible organizations, and responding to the requester.

12 SEP 2006

e. In collecting the information requested by the individual, the NAVPERSCOM PA Coordinator will send a copy of the request to the responsible office point of contact (POC), who will then search and forward the material requested.

(1) If access has been requested, arrangements will be made to make material available at a specified time.

(2) If copies have been requested, the responsible office will make the copies and send them to the NAVPERSCOM PA Coordinator. The material must be screened to ensure that the privacy of other individuals is maintained. For example, a message filed in the individual's record that contains data concerning several individuals must be photocopied so the names of all individuals except the subject of the record are blocked out. Office POCs are strongly encouraged to bring any records to the NAVPERSCOM PA Coordinator where there is a question of what should or should not be copied. Office contacts are reminded that there are few exemptions for withholding any records from the requesting individual.

(3) If any material appears to be covered by an exemption, the NAVPERSCOM PA Coordinator will review the material in question for a final determination.

#### 11. Requests for Amendment

a. Routine requests for error correction and changes to records not involving the PA should be processed according to other current procedures. The PA Coordinator should not become involved in the normal, day-to-day operations of the organization.

b. If any Department receives a request to change, amend, or delete any record, document, or data element, and the PA is invoked, the request must be hand-carried, mailed, or e-mailed to the NAVPERSCOM PA Coordinator immediately. (Time constraints on processing amendment requests are extremely critical.)

c. The NAVPERSCOM PA Coordinator will process amendment requests. When a request for amendment has been received the request will be sent to the NAVPERSCOM PA Coordinator for the initial determination as to whether or not the amendment request can be granted.

1 2 SEP 2006

(1) If additional documentation is not required and the decision is to grant the amendment, the amendment will be made. The NAVPERSCOM PA Coordinator will ensure that the amendment is made. When the amendment has been made, a copy of the completed action will be completed, signed, and returned to the NAVPERSCOM PA Coordinator by the due date specified. Extensions cannot be granted except in extreme circumstances due to the critical time constraints imposed by the Act.

(2) If additional documentation or clarification is required to process the request or amendment, provide a statement requesting same in finished format, along with the request to the NAVPERSCOM PA Coordinator for inclusion with response to the requester.

(3) If the responsible office determines that the amendment requested will not be granted, this should be conveyed back to the NAVPERSCOM PA Coordinator in writing (with the reasons and citations of existing instructions supporting the determination not to amend).

## 12. Release of Information and Accounting of Disclosures

a. Previous regulations concerning the release of information from the personnel records of members and former members of the naval service permitted disclosure of certain personal information when a specific purpose under those regulations was stated. In many instances, these disclosures are no longer permitted by the Privacy Act of 1974 without the written consent of the individual. Any department receiving such an inquiry should consult the NAVPERSCOM PA Coordinator.

b. Generally, information can be released on a need-to-know basis to other organizations within DOD.

c. Duty officers generally should not divulge information from personnel records. Few requests for such information are so urgent that they cannot be held for processing through established channels during the next working day. In any event, FOIA-type information only will be released.

d. An accounting of each disclosure of information from an individual's record must be recorded and maintained unless either of the following conditions applies:

1 2 SEP 2006

(1) The information is released to officials and employees of DOD (if the need-to-know is established).

(2) The information is requested and releasable under the FOIA (e.g., for information normally releasable to the public.)

e. Generally, an accounting of disclosures of personnel record information outside DON or DOD, even to a routine user as published in Record Systems Notices, requires an accounting of the disclosure. Enclosure (2) is to be used for manually maintained records.

f. If, however, there is an ISSA between organizations and another agency (e.g., Department of Veterans' Affairs), then the exchange of personal information (e.g., verification of service for veterans' benefits) is considered to be an intra-agency disclosure.

### 13. Statement of Dispute

a. If denial of a request for amendment is upheld through the review process, the individual is entitled to file a statement of dispute with the PA System Manager setting forth the reasons for the individual's disagreement with the refusal of the agency to amend the record.

b. The record (including computer data elements) must be clearly annotated so the fact that the record is disputed is apparent to anyone who may subsequently access, use, or disclose it. The notation itself should be integral to the record and specific to the portion in dispute. Computer files may be cross-referenced to a paper statement of dispute on file.

c. When the record or portion of the record to be disclosed is the subject of a statement of dispute, it must be noted that the information is disputed and a copy of the individual's statement provided to the user. Also, to the extent an accounting of disclosures was maintained, a copy of the statement dispute must be sent to prior recipients of the record or portion of the record involved.

d. Specific procedures for processing statements of dispute will be issued separately.

13 SEP 2006

14. Form. OPNAV 5211/9 (Mar 92), Disclosure Accounting Form is available online at <http://forms.daps.dla.mil/order/>.



MURRAY W. ROWE

Deputy,

Commander Navy Personnel Command

By direction

Distribution:

Electronic only via BUPERS Web site

<http://www.npc.navy.mil/ReferenceLibrary/Instructions/>

1 2 SEP 2006

**RULES OF CONDUCT UNDER THE PRIVACY ACT**

1. Maintaining Personnel Records. It is unlawful to maintain systems of records about individuals without prior announcement in the Federal Register. Anyone maintaining these records is subject to criminal penalties up to \$5,000. Even with such notice, care will be taken to keep only the personal information necessary to do what the law and the President, by executive order, require. The information is to be used only for the purposes described in the Federal Register.
  
2. Disclosure. Information about an individual will not be disclosed to any unauthorized individuals. Anyone who makes an unauthorized disclosure on purpose may be fined up to \$5,000. Every member or employee of the Department of the Navy who maintains records about individuals has an obligation to do their part in protecting personal information from unauthorized disclosure. SECNAVINST 5211.5E describes when disclosures are authorized.
  
3. Individual Access. Every individual, with certain exceptions, has the right to look at any PA record the Department of the Navy keeps on them, to copy it, and to request to have it corrected if they consider it wrong. The individual attempting to exercise these rights will be given courteous and considerate assistance.
  
4. Ensuring Accuracy. The Department of the Navy has an obligation to use only accurate, timely, relevant, and complete information when making decisions about individuals. Every member, official, and employee involved in keeping records on individuals will assist in the discharge of this obligation.

# DISCLOSURE ACCOUNTING FORM

## RECORD OF DISCLOSURE

**UNAUTHORIZED DISCLOSURE OF PERSONAL INFORMATION FROM  
THIS RECORD COULD SUBJECT THE DISCLOSURE TO CRIMINAL PENALTIES**

1. This is to remain a permanent part of the record described below.
2. An entry must be made each time the record or any information from the record is viewed by, or furnished to any person or agency, except:
  - a. Disclosure to DOD or DON personnel having a need to know in the performance of their official duties.
  - b. Disclosure of items listed in paragraphs 13b(2)(a) and (f) of SECNAVINST 8211.5 series.

**TITLE & DESCRIPTION OF RECORD**[illegible]

**OPNAV 5211/9 (MAR 1992)**